

IN THE UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO

ORANGEBOY, INC.,  
11 E. Gay St., 2<sup>nd</sup> Floor  
Columbus, OH 43215

Plaintiff,

v.

PATRON POINT, INC.,  
Ohio Registered Agent Service, LLC  
6545 Market Ave. North, #100  
North Canton, OH 44721

and

DOES #1–5,

Defendants.

Case No. \_\_\_\_\_

Judge \_\_\_\_\_

**COMPLAINT**

Now comes plaintiff OrangeBoy, Inc. (“OrangeBoy”), and for its complaint against Patron Point, Inc. (“Patron Point”) and Does #1–5 (collectively, “Defendants”) alleges as follows:

**PRELIMINARY STATEMENT**

1. Plaintiff OrangeBoy is the target of a coordinated effort by Patron Point, a direct competitor, and Does #1–5, unknown persons acting in concert with Patron Point, to breach the security of OrangeBoy’s computer systems, potentially exposing millions of third parties’ privacy information, violating their privacy and irreparably harming OrangeBoy’s business in the process. Patron Point has repeatedly tried to guess and reset passwords for user accounts belonging to OrangeBoy and to its clients. It has also used an “email subscription bomb” to sign up OrangeBoy users for thousands of email subscriptions, in an apparent effort to hide its

password-guessing attempts in a flood of other messages. And it has employed a fake identity, claiming to be a potential client and asking to see nonpublic information about OrangeBoy's technology.

2. So far, these efforts have failed to breach OrangeBoy's security. Even so, they have caused OrangeBoy substantial harm through having to defend, investigate, and respond to Defendants' attacks. More to the point, these fraudulent and illegal efforts risk causing irreparable harm, not just to OrangeBoy, but also to the clients and third parties who trust and rely on OrangeBoy to protect their private information.

3. Though OrangeBoy has reached out to Patron Point in an effort to resolve this matter amicably, to date Patron Point has given OrangeBoy no reason to believe that this improper and illegal conduct will stop.

4. OrangeBoy therefore brings this action to put an end to—and as much as possible, to remedy—Defendants' unlawful conduct.

### **PARTIES**

5. Plaintiff OrangeBoy, Inc. is a corporation organized and existing under the laws of the State of Ohio. OrangeBoy does business and has its principal place of business in Franklin County, Ohio.

6. Defendant Patron Point, Inc. is a corporation organized and existing under the laws of the State of Ohio. Patron Point does business and has its principal place of business in Franklin County, Ohio.

7. OrangeBoy does not know the true name, capacity, residence, or citizenship of Defendants Does #1–5, and so sues these persons or entities under a fictitious name. Does #1–5 have participated with Patron Point in the wrongful conduct described below. OrangeBoy will amend its complaint to more fully identify these parties when it is able.

## **JURISDICTION AND VENUE**

8. This Court has jurisdiction over the claims raised in this action pursuant to 28 U.S.C. §§ 1331 and 1367.

9. This Court has personal jurisdiction over Patron Point because it is a resident of Ohio and because this action arises from its tortious actions in this state, from its tortious actions outside this state combined with its persistent course of conduct in this state, and from its commission of criminal acts causing tortious injury with at least one element taking place in this state.

10. This Court has personal jurisdiction over Does #1–5 because this action arises from their tortious actions in this state, from their tortious actions outside this state combined with their persistent course of conduct in this state, or from their commission of criminal acts causing tortious injury with at least one element taking place in this state.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1) and (2), because Patron Point has its principal place of business in this judicial district, and because these claims for relief arise out of activity conducted by Defendants in this judicial district.

## **FACTS**

### **A. OrangeBoy's Business.**

12. Since 1996, OrangeBoy has provided consulting, analytics, and strategic-planning services to social-service and governmental entities, in particular public libraries, across the United States and Canada.

13. Today, OrangeBoy's services are centered around its software platform, known as Savannah. Savannah is a web-based software platform that helps OrangeBoy's library clients to glean insights from their operations data through advanced analytics and business intelligence reports. Savannah helps these clients act on those insights to improve their services offerings,

build deeper relationships with their customers (typically, library cardholders), secure new customers, and increase philanthropic giving through targeted email communications and feedback mechanisms. Over 125 public libraries in the United States and Canada currently use Savannah to gain meaningful insights about their operations and user bases, to communicate with their cardholders, and to gather feedback about their operations, programs, and interventions.

14. As a web-based platform, Savannah is not installed on users' computers like traditional software. Rather, OrangeBoy partners with Microsoft to operate servers in the United States and Canada to securely host the Savannah software, back-end functionality, and client databases. This allows users to access Savannah's functionality and real-time analyses at any time, from any place, so long as they have access to the Internet and a standard web browser.

15. OrangeBoy takes the security of its software platform very seriously. Not only do OrangeBoy's clients trust OrangeBoy with data about their internal operations, but in many cases they also use Savannah to engage with their own clients—library cardholders and other users of library services. To do this, these clients trust OrangeBoy with certain information about those cardholders, such as names, email addresses, and other contact information. All told, OrangeBoy is responsible for securely storing information associated with more than 35 million library cardholders across North America.

16. OrangeBoy's clients rightly expect OrangeBoy to keep this information safe and confidential. Because OrangeBoy's clients are typically governmental bodies, they are often subject to even more stringent data-security and privacy laws than private businesses would be. In any event, a security breach exposing this information to third parties could put these libraries' end-users at risk of identity theft and violate their expectations of privacy.

17. Such a security breach would be a disaster for OrangeBoy, not only subjecting it to potentially enormous legal liabilities, but more importantly causing irreparable harm to OrangeBoy's reputation. Indeed, the reputational harm caused by a security breach would likely affect all businesses in the library-services industry by destroying trust in their ability to keep cardholder data secure.

18. OrangeBoy therefore goes to great effort to ensure that its systems are secure and that its users' data remains safe and confidential. It stores user data in independent, secure databases, anonymizing or pseudonymizing it wherever possible and ensuring that all transfers are made by secure means. OrangeBoy then limits access to that data, and to Savannah more generally, by assigning user names and passwords to authorized users and requiring that each user provide appropriate credentials before they are allowed into the system.<sup>1</sup> And it regularly monitors its systems for vulnerabilities and attacks.

**B. Patron Point.**

19. Patron Point offers marketing-automation software to libraries in Ohio and other states in competition with OrangeBoy. Though its software does not include counterparts to all of the functionality provided by Savannah, the company claims to offer the same or similar services to Savannah at a lower price.

**C. OrangeBoy observes attempts to breach its security and links those attacks to Patron Point.**

20. On June 2, 2020, OrangeBoy detected an attempted attack on its system. That afternoon, someone used Savannah's "Forgot Password" page to try to reset the Savannah

---

<sup>1</sup> Indeed, OrangeBoy encourages clients to use "two-factor authentication," which provides more security by requiring users to enter not just a password, but also a second piece of information (such as a security code provided over text message or by an application on the user's smartphone) before they are given access to Savannah.

passwords for several OrangeBoy email addresses, including that of the company's President, Sandy Swanson. Around the same time, someone submitted fake information to a contact form on OrangeBoy's web site, seeking a demonstration of Savannah.

21. These efforts to gain access to Savannah did not succeed. Nevertheless, OrangeBoy initiated an investigation into the attack.

22. As part of its investigation, OrangeBoy attempted to trace the IP address of the attacker. Internet Protocol addresses, more commonly known as IP addresses, are unique numbers assigned to each device connected to a computer network, such as the Internet. They are used to identify computers on a network and to route communications to the correct recipients. Although sophisticated attackers often hide their true IP address by routing their actions through various third parties, in certain situations IP addresses can be traced back to particular persons or computers, or to certain parts of the world.

23. OrangeBoy determined that the IP address of the person who tried to reset OrangeBoy's passwords originated from Johnstone, Scotland, a town near Glasgow.

24. Later in its investigation, OrangeBoy performed an exhaustive search of its activity logs to see if the attacker's IP address appeared elsewhere. One entry came up, showing that on January 17, 2020, the same Scotland-based IP address had tried to log into Savannah using the email address "scott.euan.downie@gmail.com."

25. This caught OrangeBoy's attention, because the person using this IP address appeared to share a last name and location with Patron Point's Vice President of Growth, Ian Downie, who lives in or near Glasgow, Scotland.

26. Around this time, OrangeBoy had noted that Patron Point appeared to be ramping up its efforts to compete with OrangeBoy. Among other things, it had begun sending emails to

OrangeBoy clients comparing its product favorably to Savannah, and it had bought advertisements on Google to show up when users searched for “OrangeBoy,” “orange boy,” and similar terms.

27. In late July, another attack on OrangeBoy’s security drew closer scrutiny.

28. This attack had three parts. First, on July 29, 2020, someone using the IP address 209.58.142.156 initiated an email subscription bomb against five OrangeBoy email addresses. An “email bomb” is an attack that sends an extremely large number of messages to an email address. In this case, the five OrangeBoy email addresses were signed up for over 10,000 email subscription lists.

29. Email bombs are a type of “denial of service” attack used to overwhelm the victim’s email system by flooding it with more messages than it can handle. At their worst, email bombs can make the target’s email service completely unusable, but even milder attacks such as the one here slow down email delivery and impair the availability of the service. Moreover, email bombs can work to impair hide nefarious activity by burying an important email—such as a fraud alert, an illicit purchase confirmation, or a password-change notification—in a flood of unimportant messages.

30. Just so here. Shortly after the email subscription bomb began, the same IP address that initiated the attack began trying to guess (and in some cases, to reset) the passwords of several different Savannah users. Notably, these efforts to gain access to Savannah were not limited to OrangeBoy users; rather, this time the attacker tried to guess passwords associated with OrangeBoy’s *clients*.

31. Around the same time, someone impersonating a potential client began seeking nonpublic information about Savannah. This person filled out a form on OrangeBoy’s web site

claiming to be “Sara Mortimer” from the “Saint Paul Library.” “Sara” asked for information about how Savannah handles messaging to library users. After OrangeBoy’s Sales Manager answered her initial question, “Sara” responded with additional, more detailed requests. OrangeBoy’s Sales Manager offered to set up a phone call to discuss further, but “Sara” declined, claiming that she was “on the Front Desk today.”

32. Later, after “Sara” asked for access to a demo site, OrangeBoy’s Sales Manager again offered to schedule a time to talk. “Sara” again declined, claiming that she was on vacation the following week and asking for additional information that she could peruse during that vacation. This email, however, did not come from the “stpaullibrary@outlook.com” email address that the rest of the conversation had used. Instead, the email account sending this last message from “Sara” was listed as “Beth Ryan <beth.ryan100@gmail.com>.”

33. On further investigation, OrangeBoy determined that “Sara Mortimer” was using the same IP address as the person who initiated the email subscription bomb and who had been trying to guess Savannah passwords. This finding triggered further investigation from OrangeBoy’s security team.

34. OrangeBoy’s investigation has thus far failed to determine the identity of “Sara Mortimer.” None of the “St. Paul” libraries in the United States and Canada has been able to confirm that they employ a person with that name, and social-media searches turn up no useful information about “Sara Mortimer.”

35. OrangeBoy has discovered, however, Twitter accounts that appear to be connected to this attacker. One such account is named “St Paul Public Library” (<https://twitter.com/StPaulPublicLi1>) and the other is named “Beth Ryan” (<https://twitter.com/BethRya37389413>). Both accounts were created in May 2020, and both accounts’ only activity



since they were created has been to retweet numerous marketing messages from Patron Point's corporate account. Neither account has shown any activity since OrangeBoy confronted Patron Point about the attacks on its system.

36. Moreover, OrangeBoy investigators noted that shortly before the attacks began on July 29, its web site had been visited by IP addresses that traced back to Wilmslow, England, and to Johnstone, Scotland. Patron Point's Business Development Director, Nigel Wheeldon, lives in or near the town of Wilmslow, England. And as noted above, Patron Point's Vice President of Growth, Ian Downie, lives near Johnstone, Scotland. OrangeBoy does not provide services to any libraries in the United Kingdom; it does not market Savannah in the United Kingdom; and based on past web site traffic, this pattern of visitors from the United Kingdom—let alone from areas connected to Patron Point employees—is abnormal.

**D. Patron Point has failed to take steps to stop and prevent these attacks.**

37. On August 3, after having determined that Patron Point appears to be behind these attacks, OrangeBoy sent Patron Point a letter demanding prompt action. Exhibit A to this Complaint is a true and correct copy of this letter.

38. In the more than two weeks since OrangeBoy sent that letter, Patron Point's counsel has repeatedly assured OrangeBoy that it is investigating the matter. To date, however, the company does not appear to have taken any steps to stop or prevent future attacks or efforts to undermine OrangeBoy's security.

39. In light of the increased sophistication of the most recent round of attacks, as well as Patron Point's failure to respond substantively to OrangeBoy's correspondence, OrangeBoy feels compelled to take legal action to ensure the continued security of OrangeBoy's system and its clients' data.

**COUNT I**  
**(Computer Fraud and Abuse Act, 18 U.S.C. § 1030)**

40. OrangeBoy incorporates and realleges the preceding paragraphs as if fully set forth herein.

41. Patron Point and Does #1–5 intentionally tried to gain access to OrangeBoy’s Savannah software by, among other things, attempting to guess the passwords of authorized users of that software, using fake names and credentials to try to acquire nonpublic information about the software, and signing up OrangeBoy users to thousands of unwanted email subscriptions to cover up their efforts.

42. Defendants took these actions knowing that they did not have authorization to access OrangeBoy’s Savannah software.

43. As a result of Defendants’ conduct, OrangeBoy has suffered damage and loss of at least \$5,000 in value, including the impaired availability of its email system and the cost of investigating and responding to the attacks.

44. Moreover, if Defendants’ efforts to breach OrangeBoy’s security had succeeded, OrangeBoy would have suffered substantially higher losses. Such losses would be at least partly irreparable, as a successful breach of OrangeBoy’s security would cause damage to OrangeBoy’s reputation, goodwill, and industry standing that could not be fully quantified and compensated through money damages.

**COUNT II**  
**(Unfair Competition)**

45. OrangeBoy incorporates and realleges the preceding paragraphs as if fully set forth herein.

46. Patron Point has engaged in a pattern of unfair commercial practices, committing acts that are unlawful, unfair, deceptive, and/or fraudulent in an effort to harm OrangeBoy's business.

47. As a result of Patron Point's conduct, OrangeBoy has suffered damages.

48. Patron Point's unfair commercial practices further risk doing irreparable harm to OrangeBoy's business, not only through threatening to breach OrangeBoy's security, but also through its efforts to use fake names and institutional affiliations to obtain confidential and proprietary information about OrangeBoy's technology.

**COUNT III**  
**(Injuries from a Criminal Act, Ohio Rev. Code 2307.60)**

49. OrangeBoy incorporates and realleges the preceding paragraphs as if fully set forth herein.

50. By the conduct described above, Patron Point and Does #1–5 committed criminal acts, including violations and attempted violations of Ohio Revised Code 2913.04; Ohio Revised Code 2913.05; 18 U.S.C. § 1030; and 18 U.S.C. § 1832.

51. Defendants' criminal acts have harmed OrangeBoy.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff OrangeBoy, Inc. respectfully requests that this Court enter judgment in its favor and issue the following relief, as applicable:

1. Temporary, preliminary, and permanent injunctive relief barring Defendants, and anyone working for, with, or in concert with them, from:
  - a. Seeking unauthorized access to OrangeBoy's computers, systems, or platforms;
  - b. Signing up OrangeBoy users for unwanted email subscriptions or otherwise disrupting OrangeBoy's information technology systems; and

- c. Using false names or institutional affiliations to seek nonpublic information about OrangeBoy's technology;
2. Monetary damages, including treble damages as appropriate under Ohio Revised Code 2307.61, in an amount to be proven at trial;
3. An award of punitive and exemplary damages;
4. Reasonable costs and expenses, including attorneys' fees; and
5. Such other relief as the Court deems just and proper.

Dated: August 20, 2020

/s/ Joshua M. Feasel  
Joshua M. Feasel (0090291)  
Feasel PLLC  
P.O. Box 6842  
Detroit, MI 48202  
734.726.0016  
313.217.3509 (f)  
jmfeasel@feaselpllc.com

*Attorney for Plaintiff OrangeBoy, Inc.*

**JURY DEMAND**

Plaintiff OrangeBoy, Inc. demands a trial by jury on all claims.

Dated: August 20, 2020

/s/ Joshua M. Feasel  
Joshua M. Feasel

*Attorney for Plaintiff OrangeBoy, Inc.*